Securely Connecting the World with Cyber Security Standards

by

Alicia Clay and Michael D. Hogan

National Institute of Standards and Technology

Introduction

"Over the course of a few years, a new communications technology annihilated distance and shrank the world faster and further than ever before. A worldwide communications network whose cables spanned continents and oceans, it revolutionized business practices and gave rise to new forms of crime." [1]

Our first experience with revolutionary changes brought about by on-line technology that improved connectivity is more than 150 years old. The telegraph was able to revolutionize the way we communicated and hence the way we fostered business and personal relationships not simply because of the technological advances but because we were able to standardize the way in which those advances were applied. Similarly, nineteenth century trains gave us physical mastery over distances that we had not seen before. The nineteenth century trains also highlighted the impact of standards on connectivity. Over the course of two days in 1886, the rails were moved on over 11,000 miles (17,600 km) of railroad tracks stretching from Virginia to Florida to Texas. They were changed to the standard 4-foot 9-inch (145 cm) width used by the rest of the nation. This eliminated the considerable costs of reloading cars and changing wheels between the South and the rest of the nation. It was a Herculean effort that shaped both commerce and lives as goods and families moved more easily by rail.

Like railroads and the telegraph, the Internet has brought us to the brink of yet another step function increase in connectivity and perhaps to the brink of a revolutionary change in how we live and work. We are still exploring the possibilities afforded by being always on and always connected. As with the rail system, however, there is a great need to standardize network interfaces and interconnections so that exchanges across networks aren't corrupted or stalled. Technologies that connect us work because of standards. These technologies however have been both a blessing and a curse. Technological innovation, while enabling new businesses and modes of business, opens the door to new threats. Standards are also the vehicle by which things can be made to work securely. Developing the standards to support the connected world of the Internet and Web has been arduous but, so far, successful. Increases in connectivity have lead to great advancements, new forms of crimes, and increased difficulty in fighting crime.

---

[1] The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers, by Tom Standage, 1999

Standards are the key to seeing the full benefits of our enhanced connectivity and to stemming the new threats that have accompanied this connectivity. A major challenge will be to develop timely standards to defeat these threats. This paper focuses on some of the key roles that cyber security standards play in securely connecting our cyber world.

Cyber Security Standards

By standards, we mean documentary standards[2] as well as measurement and testing standards. Cyber is an adjective frequently used to refer to computers and networks. Finally, by security, we mean all attributes of security, which include:

- Confidentiality (of data and system information)
- Integrity (of systems and data)
- Availability (of systems and data for intended use only)

Confidentiality ensures that information is not disclosed or revealed to unauthorized people. Integrity ensures consistency of data by preventing unauthorized creation, alteration or destruction of data. Availability ensures that legitimate users are not unduly denied. Availability is sometimes cast in its opposite sense - "denial-of-service." Internet failures from malicious hackers are an ongoing, highly publicized example of "denial-of-service." Ultimately one must have assurance that the objectives of security have been adequately met. The interdependencies inherent in these security attributes are illustrated in Figure 1.

[2] Standard (norme) - Document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. Note - Standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits. - *ISO/IEC Guide 2, Standardization and related activities - General Vocabulary*

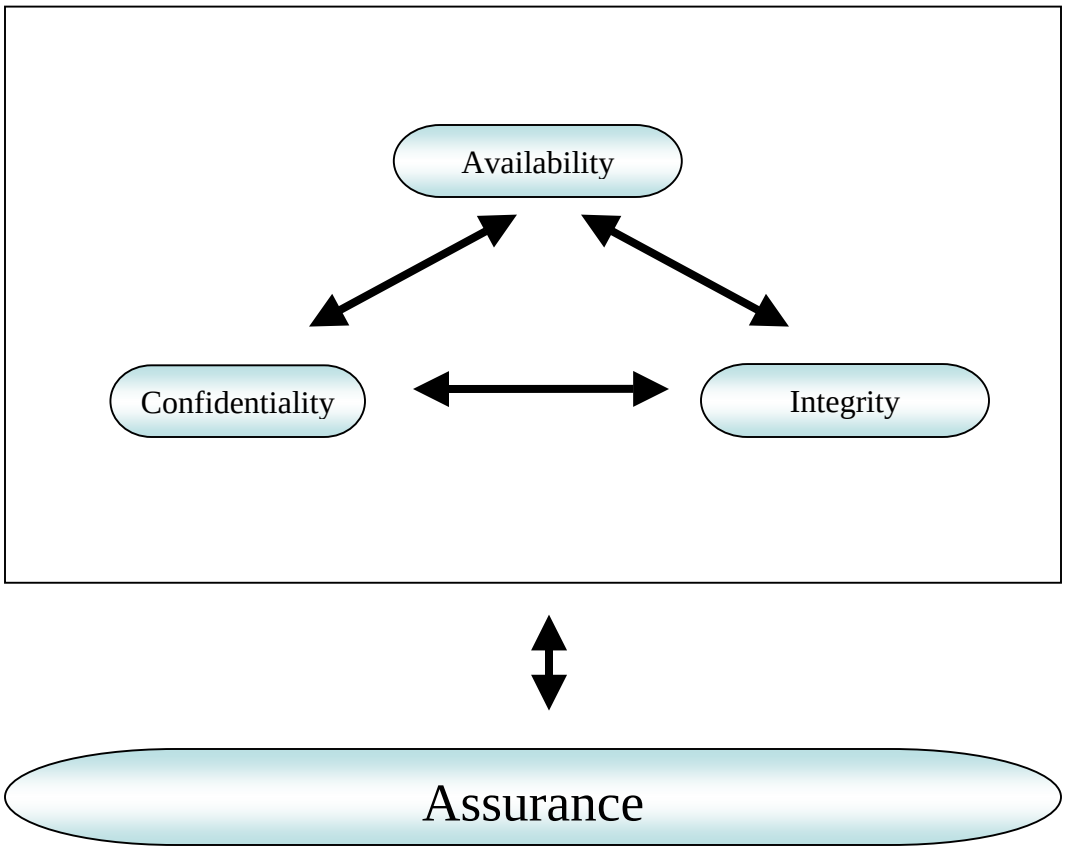

Figure 1: Dependencies of Security Attributes

Cyber security is in its infancy. Less than 35 years ago, the concept of remotely interconnected systems began with the connection of four university mainframes. [3] In 1971 the first email program was created to send messages across a distributed network. In 1980 an accidentally propagated status message caused the first denial of service "attack", bringing down the burgeoning system.[4] Today there are more than two million Internet hosts with 840 million users. The Computer Security Institute and the FBI estimate that businesses loss more than $140 million to information security breaches last year.[5] Public and private sector organizations around the world are attempting to stop this hemorrhaging by establishing practices for maintaining cyber security. The vast diversity in both the form and function of systems and the means by which they are connected makes securing such systems almost as difficult as connecting them. It does not help that it is widely accepted that every system is breakable given enough time and

[3] http://www.cbc.ca/news/background/internet/
[4] http://www.zakon.org/robert/internet/timeline/

resources. As more and more of these systems are used to support business transactions and critical infrastructure, system owners are called to show due diligence in their security planning. Again this is a challenge since one to one correlations have not yet been made between security controls and threats. Without being able to parallel the relationship that sprinklers have to fire damage, system owners are called upon to calculate return on investment for their security initiatives. This is the point where cyber security standards built by consensus of a variety of stakeholders can give us a great advantage. By pooling the knowledge and experience of system designers, practitioners and end users, standards are being developed which provide a path for effective and secure connectivity. As we become accustomed to the benefits of being always on and always connected, of just in time products and services, the need for open, international voluntary consensus standards will grow exponentially. These standards will be necessary to support acceleration of the deployment of significantly better standards-based security solutions in support of global business and new homeland security priorities.

Categories of Cyber Security Standards

Cyber security standards can be categorized as technical, management, or testing standards. All three types of standards are necessary to achieve the objectives of cyber security. Technical standards typically give normative requirements for an information system's hardware, software, or firmware to assure interoperability and to protect the system and its information from unauthorized access, use, disclosure, disruption, modification, or destruction. Examples would include standards for role based access control, Internet protocol architecture, and encryption algorithms. Management standards typically dictate the means by which an organization is expected to manage the security of the information system and the associated risk to the organization's assets and operations. Examples include standards on security categorization of information systems, security self-assessment, and principles and practices for securing systems. Testing standards typically describe testing methodologies and the means by which an organization is directed to verify that a system or its components is functioning as expected. Examples include standard tests for conformance, interoperability, assurance, functionality or standard measures of performance against stated capabilities.

[5] http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

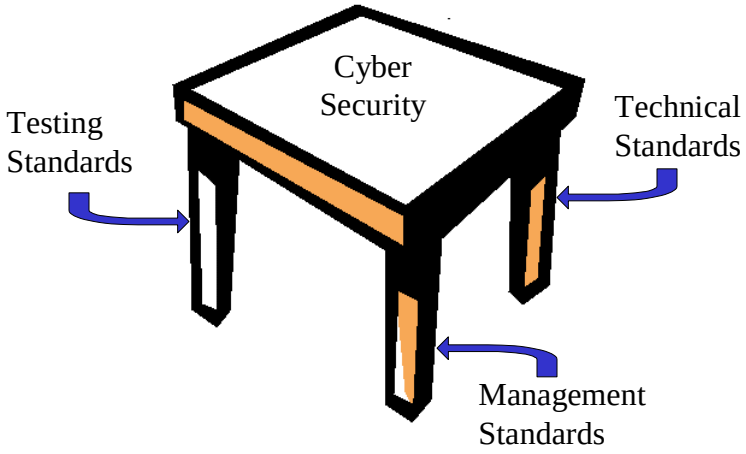

Figure 2: Categories of Cyber Security Standards Essential for Cyber Security

Hot Areas for Cyber Security

Web-based business models are impacting all areas of commerce and society. We are on our way towards eEverything (healthcare, banking, retail sales, business supply chains, education, manufacturing, government services, etc.). The really big bumps in the road are those of security. Threats include attacks from within (disgruntled employees), attacks from without (viruses, worms), identity theft, loss of privacy, spyware, and spam, to name a few potentially catastrophic to merely annoying problems. These threats endanger the security of our society because they endanger the networks upon which our society is becoming more and more dependent. Cyber threats and crimes will not be controlled without timely development and widespread use of comprehensive, quality cyber security standards. Three challenges key to preventing cyber based crimes of connection are identity management, cyber security testing, and secure management of information systems.

Identity Management

Identity management entails authoritative sources in organizations issuing identifiers for persons (employees, customers, residents, etc.). These authoritative sources rely upon references and support in the form of government issued identification such as birth certificates, driver's licenses, and passports. Unfortunately phony credentials remain all too easy to obtain. This problem is compounded by the connectivity and anonymity cyber space.

The need for identifier management is readily apparent in the crime of identity theft. Identity theft is defined as all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. Identity theft inflicts substantial costs on both individuals and businesses. According to the U.S. Federal Trade Commission (FTC), from May 2002 to April 2003, an estimated 10 million Americans became identity theft victims. Other statistics reported by the FTC:

- Average loss per victim of identity theft: $4,800
- Average amount victims spent to resolve problems associated with identity theft: $500
- Average amount of time spent by victims to clear up affairs: 30 hours
- Total annual cost of identity theft to victims: $5 billion
- Average value of money or goods obtained by criminals using a victim's personal information: $10,200
- Total annual loss to businesses, including financial institutions, from identity theft: $48 billion

Couple these statistics with the fact that the anonymity of the Internet allows one to easily assume an identity – any identity or no identity – and instigate or corrupt any number of transactions and the problems inherent in identity management are clear.

There is now the potential to eliminate current types of identity theft through the use of standards-based biometric and smart card technologies. Biometric technologies use personal characteristics to automatically identify and verify persons. Some of the personal characteristics being used for recognition include fingerprint, face, iris, vein, hand geometry, signature, and voice. With biometric technologies, there is no need to remember passwords or carry documents, all of which are subject to being compromised. New and highly secure identity applications become

possible when a biometric is stored on a physical device, such as smart cards. One application is biometric/smart card based employee identification for physical and logical access control. Another application is biometric/smart card based financial transactions, replacing today's magnetic striped/password credit and debit cards. Post September 11th priorities for homeland security are now driving efforts to develop high performance interoperability standards for biometrics and smart cards. The key U.S. venues for this standardization are INCITS Technical Committees B10, for smart cards, and M1, for biometrics. In addition to developing national standards, both committees act as the U.S. technical advisory groups to subcommittees in ISO/IEC JTC 1. Since the first meeting of INCITS M1 in January 2002, many critical biometric standards have already been approved as ANSI INCITS standards and others are nearing completion. INCITS B10 has now begun work on the final piece of the interoperability puzzle for smart cards with recent projects based upon the NISTIR 6887-2003 Edition, *Government Smart Card Interoperability Specification (v2.1)*. The counterpart international standardization is underway in ISO/IEC JTC 1 SC 17, for smart cards, and SC 37, for biometrics. All of this work is crucial for successful deployments of new highly secure standards-based security solutions. Enterprise systems and applications based upon voluntary consensus biometric and smart card standards are far more likely to be interoperable, scalable, usable, reliable, secure, and economical than proprietary systems. Figure 3 shows the interrelationships of biometric based standards work in ISO/IEC JTC 1 SCs.

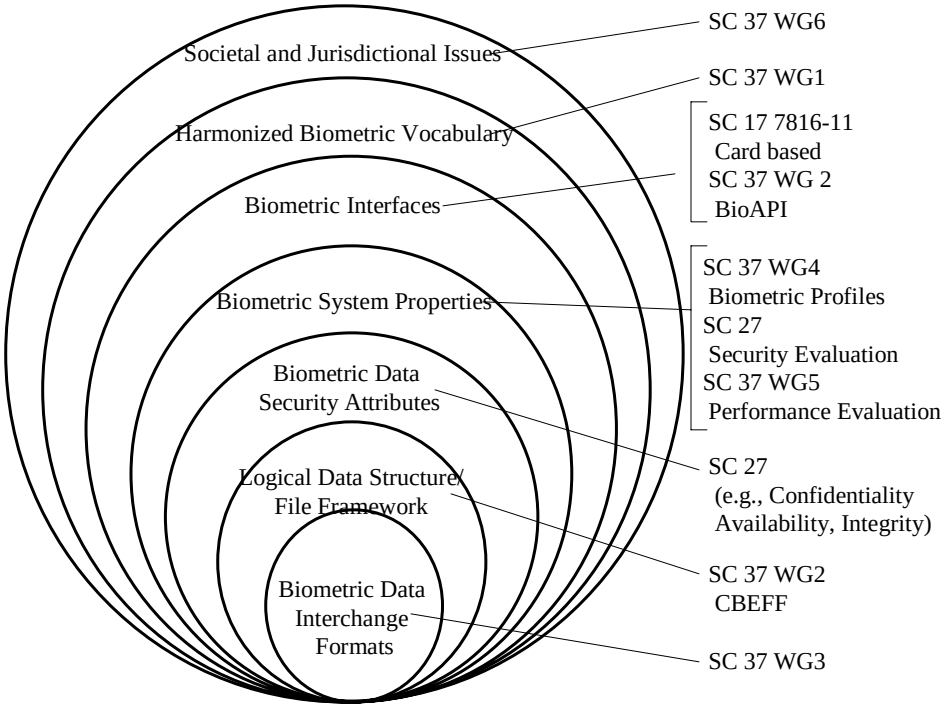

Figure 3: Biometric Standards Activities in JTC 1

With all of their advantages, biometric technologies are not the last word in security. With non-zero false acceptance and false rejection rates, they are not as reliable as some other technical controls. As relatively new technical security controls, tests for their effectiveness tend to be empirical rather than objective and mathematically quantitative as are tests for random number generators. Additionally, individuals have a finite set of unique biometric identifiers. Should an individual's fingerprint data be inappropriately shared, it cannot be "reset" like a password. Therefore biometric controls are best used in the context of appropriate management, operational and testing controls.

Cyber Security Testing

Cyber security testing requires cyber security standards that have testable specifications. Lord Kelvin[6] captured the importance of good measurements back in the nineteenth century:

[6] William Thomson, who was knighted in 1866 and was raised to the peerage in 1892 (as Baron Kelvin of Largs) in recognition of his work in engineering and physics, was foremost among the small group of British scientists who helped to lay the foundations of modern physics.

“When you can measure what you are speaking about and express it in numbers, you know something about it; but when you cannot measure, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science.” A test is a technical operation that consists of the measurement of one or more characteristics of a given product, process or service according to a specified procedure. Conformance testing captures the technical description of a specification in a standard and measures whether an implementation faithfully implements the specification. Interoperability testing consists of the testing of one implementation (product, system) with another to establish that they can work together properly.

Cyber security standards may achieve international approval and acceptance only to see this international harmonization fractured by the testing environment. There is no international body for the approval of testing. Consequently, harmonization and acceptance of testing programs is often a bilateral or multilateral exercise by the concerned testing organizations. There are actions the standards developers can take to help ensure the harmonization of testing.

Cyber security standards are almost always developed and specified in a natural language, English, which is inherently ambiguous. Sometimes the specifications in a standard are developed or translated into a more unambiguous language called a formal description technique (FDT). Since the specifications in cyber security standards are often very complex, as well as specified in ambiguous form (English), most testing methodology standards require the development of a set of scenarios, used in support of testing. Typically the standards developing organization develops the cyber security standard, the FDT specification, the testing methodology, and the test case scenarios. One or more testing organizations may develop tools such as executable versions of the test case scenarios. This may result in more than one conformance test tool being available. However, if a rigorous testing methodology standard has been adhered to, it should be possible to establish the equivalence and quality of the available test tools.

Figure 4 shows the possible modes of testing and acceptance in the marketplace. Consumers may choose to have the security of products tested in a vendor's laboratory, in the consumer's laboratory or by independently accredited

laboratories. Consumers may also choose to have the test results independently certified. However, the ultimate goal is internationally approved cyber security standards being used globally. Programs assessing conformance to cyber security standards may develop anywhere in the world. Harmonized testing, accreditation and validation programs promote trade and allow consumers the benefit of buying products in a diverse, global market.

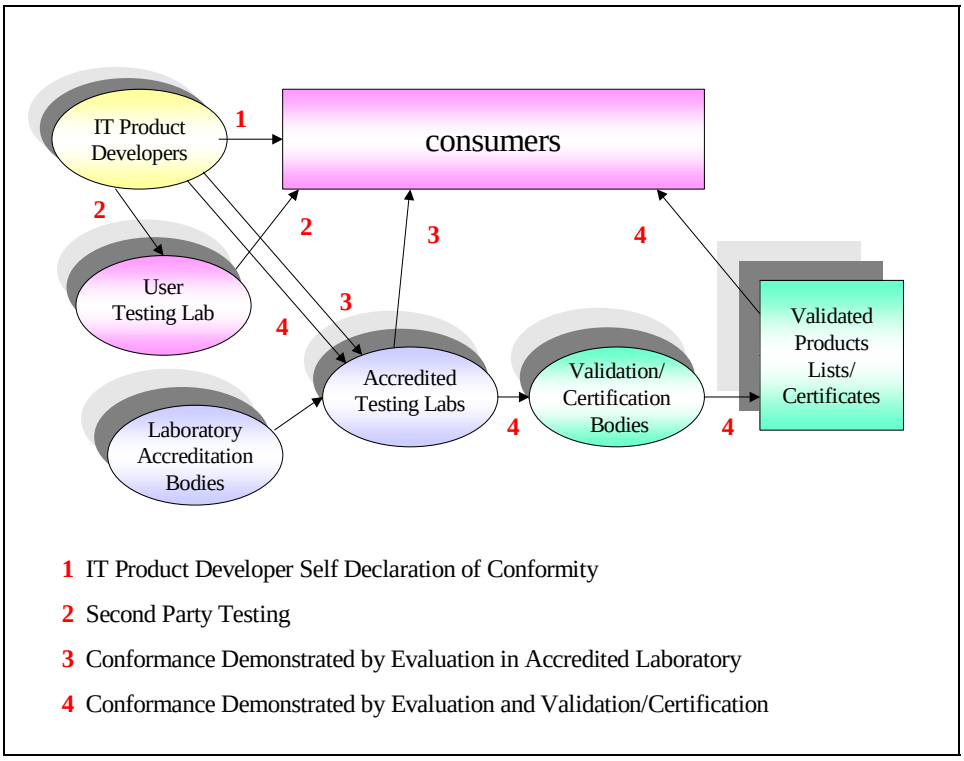

Figure 4: Possible Modes of Testing and Acceptance

In order to harmonize independently developed conformity assessment programs, organizations operating such programs will have to agree on the equivalence of their programs with respect to issues such as: base standards, conformance testing methodology standards, test tools, testing laboratories, laboratory accreditation bodies, and certification bodies. Agreement on these issues constitutes the basis for formally harmonizing through a formal memorandum of understanding. This is the key to obtaining the elusive goal: "one standard, one test report, accepted everywhere."

The best example we have of this today is the testing supported by ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation. This multipart standard is used as the basis for evaluation of

security properties of IT products and systems. The standard permits comparability between the results of independent security evaluations. This is done by providing a common set of requirements for the security functions of IT products and systems and for the associated assurance measures applied to them during a security evaluation. [7] Because of the crucial nature of cyber security, customers of cyber security testing will likely continue to prefer accredited testing and certification schemes.

Secure Management of Information Systems

The crux of cyber security lies in how security is managed within and across systems. One must take into consideration the fact that people are an integral part of all information systems. All systems require input from, send output to or are designed to support … people. Any number of technical controls can be designated in order to better secure a system or aid in contingency operations or disaster recovery. However, it is still left to people to implement said controls, and work through them rather than around them. It is also in the management and general maintenance of an information system that one can look for assurance of adequate risk assessment and due diligence in risk management. With ever increasing connectivity aimed at advanced and more efficient business interactions as well as exponential growth in options supporting life and leisure, information security management standards can be the key to safely connecting.

An information security management system (ISMS) standard would look like a standard description of the processes necessary to securely manage an information system such as (Figure 5):

- System categorization
- Risk assessment
- Security plan development
- Security control selection and implementation
- Certification of system controls and accreditation to operate
- Change management
- Periodic evaluation, review and improvement

[7] http://csrc.nist.gov/cc/Documents/CC%20v2.1%20-%20HTML/CCCOVER.HTM

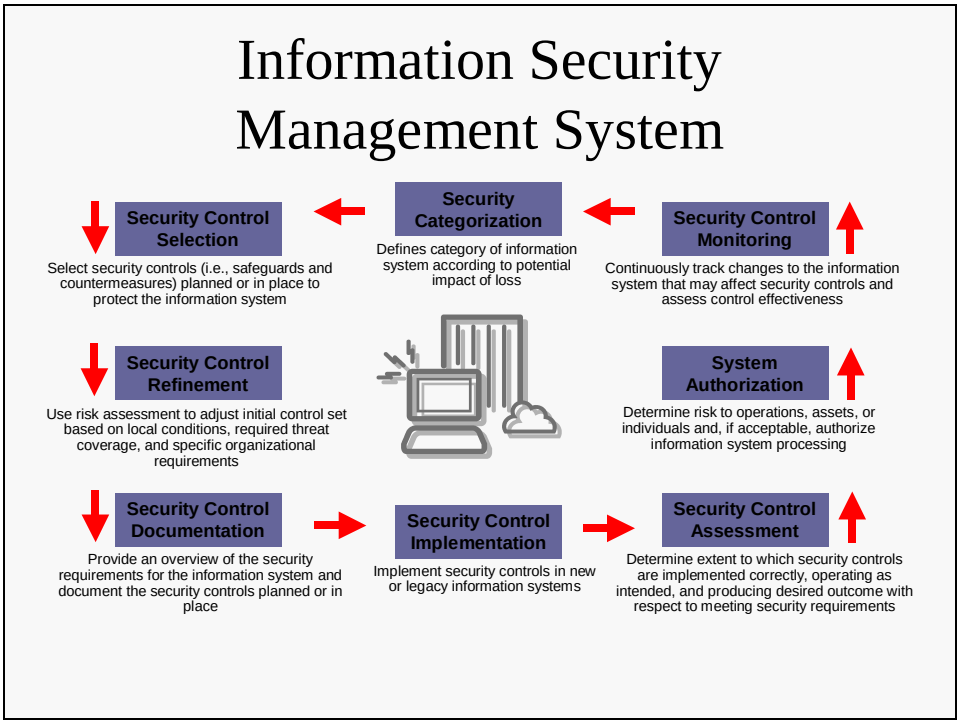

Figure 5: Sample Process for the Secure Management of Information Systems

These processes might each be detailed in individual standards and guidelines with the ISMS acting as an umbrella standard with pointers to other standards and guidelines. An ISMS would then allow flexibility of control selection and implementation based on documented, repeatable, recognized methods of risk assessment that could vary across industries, system types and operating environments. A common language and methodology for statement of risk would provide the means to verify that the ISMS processes are being run consistently and lay the groundwork for a quantitative comparison of accepted levels of risk. Thus, an ISMS standard can provide an understandable way of reporting information asset management decisions to potential partners or customers.

An effective ISMS standard should also provide a means to evaluate the output of that set of processes – namely measure the effectiveness of the information security activities, which ultimately protect an organization's information assets. This would give an indication of whether or not a specific application of the ISMS standard has adequately met the needs of the organization and would form the basis for continuous improvement. An ISMS standard with explicit requirements, methodologies and assessment tools, would also permit organizations operating

conformity assessment schemes to achieve consistent and repeatable results. Thus, a properly scoped and comprehensive ISMS standard would help build trust and confidence in information security management systems.

Several organizations are developing frameworks aimed at managing the security of information systems. Currently, ISO/IEC 17799:2000 Code of Practice for Information Security Management is the most widely recognized international standard on information security management. This standard is a guideline for the selection of security controls. The financial services community, working within ISO, has drafted a technical report with security guidelines for their sector, ISO/CD TR 13569 Banking and related financial services -- Information security guidelines. Subcommittee 27 of ISO/IEC JTC1, the home of ISO/IEC 17799, is launching a project to develop an ISMS standard and an associated standard on metrics. There is significant international support in having the ISO/IEC ISMS standard closely parallel national management standards and guidelines already in use or under development such as those in the UK, Canada, Spain and the United States. IEEE is developing a standard Information System Security Assurance Architecture. This architecture will point to a group of standards that collectively function as an ISMS. The IEEE standards will be based on the NIST framework developed to facilitate secure management of federal information systems and NIST guidelines and standards addressing system categorization, risk assessment, security plans, security control selection and implementation, and system certification and accreditation.

Developers of Cyber Security Standards

There are many organizations involved in developing cyber security standards. Some of the key national and international venues are:

- International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee on Information Technology (ISO/IEC JTC 1)
- International Organization for Standardization Technical Committee 68 on Banking and Other Financial Services (ISO TC 68)
- Internet Engineering Task Force (IETF)
- InterNational Committee for Information Technology Standards (INCITS)

- X9, Inc. - Financial Industry Standards
- Institute of Electrical and Electronic Engineers (IEEE)
- National Institute of Standards and Technology (NIST)

ISO/IEC JTC 1 develops international information technology (IT) standards required by global markets meeting business and user requirements, including the areas of security of IT systems and information interoperability of IT products and systems. JTC 1 Subcommittees (SCs) involved in standards critical to cyber security include SC 6 (public key infrastructure (PKI) certificates), SC 17 (smart cards), SC27 (generic IT security), and SC 37 (biometrics).

ISO TC 68 develops international standards in the field of banking, securities and other financial services. ISO TC 68 Subcommittee 2 (SC 2) develops international standards on security management and techniques applicable to general banking operations.

The IETF is the protocol engineering and development arm of the Internet and issues the standards and protocols used to protect the Internet and enable global electronic commerce. The IETF has over a dozen groups developing security standards for the Internet, such as Public Key Infrastructure Using X.509 (PKIX), Internet Security Protocol (IPsec), Secure Electronic Mail (S/MIME V3), Secure Network Time Protocol (SNTP), and XML Digital Signature (joint project with World Wide Web Consortium (W3C)).

INCITS is the primary U.S. focus of standardization in the field of Information and Communications Technologies (ICT) encompassing storage, processing, transfer, display, management, organization, and retrieval of information. As such, INCITS also serves as American National Standards Institute's (ANSI) designated U.S. Technical Advisory Group for ISO/IEC Joint Technical Committee 1. INCITS Technical Committees involved in standards critical to cyber security include B10 (smart cards), M1 (biometrics), T3 (PKI certificates), and T4 (generic IT security). Recently approved INCITS cyber security standards include biometric standards (ANSI INCITS 358, 377, 378, 379, 381, 383, 365) and role based access control (RBAC) (ANSI INCITS 359).

X9, Inc. is an ANSI accredited standards development committee that develops standards for the financial services industry in order to facilitate delivery of financial products and services. ANSI has designated X9, Inc. as the U.S. Technical Advisory Group for ISO TC 68. X9F (data and information security) is the U.S. counterpart of ISO TC 68/SC 2 and works with it in developing international banking security standards. Some of its key cyber security standards are signature standards (X9.30, X9.31, X9.62), key establishment standards (X9.42, X9.63), triple DES standard (X9.52), primality testing standard (X9.80), and other cryptographic algorithm standards (X9.44, X9.82, X9.92, X9.98, X9.102).

The IEEE is an international membership organization developing many key standards in the areas of computers and power. Among some of its cyber security standards projects are local area network (LAN) security (e.g., IEEE 802.11 series), Basic Operating System Security (BOSS) (P2200) and Information System Security Assurance Architecture (ISSAA) (P1700).

NIST is an agency of the U.S. Commerce Department's Technology Administration. The NIST Information Technology Laboratory (ITL) supports government agencies and the IT industry with measurements, standards, and research. Additionally, ITL is accredited by ANSI as a standards developer. In the area of cyber security, ITL develops Federal Information Processing Standards (FIPS), NIST Special Publications 800 series on computer security issues, NIST Interagency Reports (NISTIRs), and ITL Computer Security Bulletins. ITL's Computer Security Division was formed under the Computer Security Act of 1987. NIST currently operates under the mandates in the Federal Information Security Management Act of 2002 and the Cyber Security Research and Development Act of 2002. As such, NIST is responsible for developing standards and guidelines for securing all sensitive, non-classified federal systems. This includes systems owned by the federal government and systems used to support the various missions of federal agencies. Additionally, NIST guidance is frequently adopted by organizations in both public and private sector. NIST cyber security guidelines, standards and testing programs[8] are therefore used to govern a significant percentage of U.S. computer systems.

[8] http://csrc.nist.gov/

There are many other, specialized groups involved in cyber security standardization. For example, the International Telecommunications Union (ITU) focuses on cyber security from the perspective of developing standards in support of the international telephony system. The relationships between the national and international organizations mentioned herein are highlighted in Figure 6.

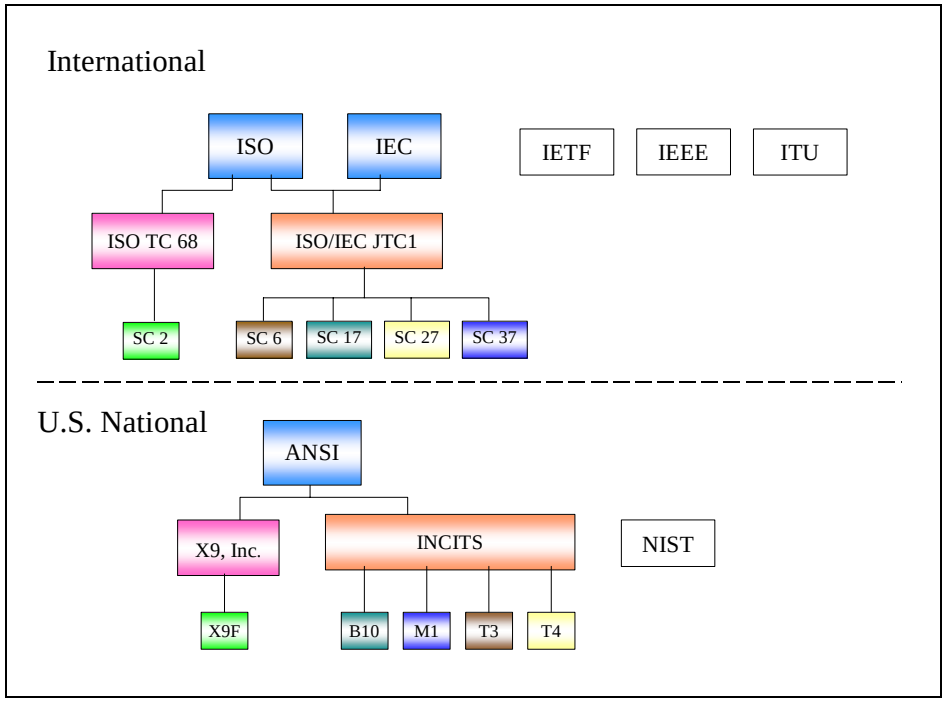

Figure 6: Cyber Security Standardization Organizations

The Way Forward to a Securely Connected Cyber World

The Internet and the Web are today's ultimate connection of the world. These advances in connectivity have been accompanied by new forms of crime. Eliminating such security threats begins with continued, successful development of timely cyber security standards. Highly secure connectivity can only be achieved by deployments of standards based products, systems, and services. To date, it has taken great efforts to develop cyber security standards and to deploy standards based solutions. This will have to continue.

Ironically, the very connectivity that often plagues us can also be a big part of the answer to better cyber security. Technical and testing cyber security standards, which assure more interoperability, can help to eliminate threats to our connectivity. For instance, emerging international standards for the interoperability of smart card and biometric technologies will support more highly secure physical and logical access. Applications for these technologies include travel documents (e.g., passports), identification badges (e.g., employees, students), and credit/debit cards. There is reason to feel optimistic about the prospects for better cyber security in the future.

However, technical and testing standards alone will not be enough to realize better cyber security. The development and use of comprehensive and sound international standards for information system security management is now the final frontier for securely connecting the world through standards. The first line of stakeholders for this work is the government and industry executives and experts responsible for cyber security in their organizations. While there are many standards developers involved in cyber security, the key international activity for information security management standards development is the ongoing work of ISO/IEC JTC 1 Subcommittee 27, IT Security Techniques. The U.S. portal for participating in this critical program of work is INCITS Technical Committee T4, Security Techniques. Presently, there are about a dozen organizations participating in T4. Given the critical importance of securely managing information systems, there should be hundreds of organizations participating in T4.

This is the challenge. In the first decade of the twenty-first century, we still need to move our "11,000 miles of railroad track."